



DEPARTMENT OF THE ARMY
MULTI-NATIONAL BRIGADE (EAST)
HQ, TASK FORCE FALCON, KFOR 6B
CAMP BONDSTEEL
APO AE 09340

S: 15 October 2005

AEKF-MNB(E)-G6

8 September 2005

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Command Policy Letter # 41 - Sensitive Information Posted to Personal Internet and "Blog" Websites

1. References:

- a. AR 25-2, Information Assurance, 14 Nov 03.
- b. AR 530-1 (Operational Security) OPSEC, 3 Mar 95.
- c. Joint Ethics Regulation, DoD Directive 5500-7R.
- d. Code of Federal Regulations, Title 5, Section 2635, Standards of Ethical Conduct for Employees of the Executive Branch.
- e. ALARACT 156/2005, SUBJECT: Chief of Staff of the Army OPSEC Guidance.
- f. ALARACT DTG: 141637Z Feb 05, SUBJECT: Sensitive Photos (U//FOUO) from General Richard A. Cody, VCSA.

2. PURPOSE. This memorandum establishes MNB (E) policy regarding the sending or posting of sensitive information via the Internet (non-secure) and posting such information on personal on-line journal sites. (Such web-sites, which frequently contain written and photographic information, are commonly referred to as "blog" sites).

3. APPLICABILITY. This policy letter applies to all military personnel assigned or attached to, serving with, accompanying, or visiting MNB (E) in either Kosovo or the Former Yugoslav Republic of Macedonia (FYROM). Supplementation of this policy requires approval of the Commander, MNB (E).

4. POLICY.

a. General Policy. Our adversaries and competitors can significantly affect the safety and capabilities of U.S. military personnel and operations through the use of sensitive and classified information that is inappropriately conveyed through the Internet. Even apparently insignificant information related to U.S. military activities, facilities, personnel, and operations may be used by our adversaries and competitors in a manner

detrimental to U.S. interests and the safety of U.S. personnel. For example, "everyday" photographs of soldiers, facilities, and equipment may provide information that can be used to determine potential vulnerabilities. Similarly, comments regarding troop movement or activities may provide insight into our operations that can be used against U.S. forces and personnel. Soldiers therefore must carefully consider operational security issues before sending or posting any electronic communication via the Internet. Additionally, soldiers may not post classified or sensitive information to blog or other Internet sites. Commanders and leaders at all levels must vigilantly ensure that our soldiers do not put our troops at risk by providing compromising information to our enemies and competitors.

b. No Use of Government Computers for Blog Sites. Soldiers are prohibited from using government owned computers to create or manage personal web or blog sites. This restriction applies to the computers located at MWR centers since they are owned by the government. As a matter of routine, computers on government networks are monitored by Information Assurance managers at all levels.

c. No Solicitation. Federal Law prohibits employees (including members of the armed forces) from soliciting or accepting a gift or other item of monetary value that is given because of the employee's official position. Employees are also prohibited from soliciting or accepting a gift or other item of monetary value from a prohibited source (i.e., any person or entity seeking official action from, doing business with, or conducting activities regulated by the employee's agency [the Department of Defense and Department of the Army], or whose interests may be substantially affected by the performance or non-performance of the employee's duties). Because it is easy, even with the best of intentions, to unintentionally violate these restrictions, soldiers are strongly discouraged from making solicitations on any blog site that they operate. In order to avoid ethics violations, all military personnel to whom this policy applies **MUST** obtain written approval from their individual commander and the Judge Advocate Ethics Counselor prior to making a solicitation for a gift or other item of monetary value on any site operated or managed by the soldier if that site contains any connection or reference to the soldier's official position or military component.

d. Briefing Requirements. Commanders will ensure that all soldiers in their command are briefed on the terms of this policy. Suspense for completion of this action is **15 OCT 05**.

5. This policy is punitive. Any soldier who posts sensitive or classified information or pictures to any Internet or blog site may receive non-judicial punishment, court-martial, and/or adverse administrative action. Similarly, soldiers who fail to comply with paragraph 4a, 4b, and 4c may receive non-judicial punishment, court-martial, and/or adverse administrative action.

6. Soldiers with questions regarding whether or not it is appropriate to convey particular written, photographic, or other information via any forum, electronic or otherwise, should seek guidance from their chain of command prior to doing so.

AEKF-MNB(E)-G6

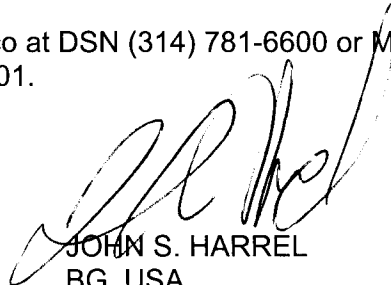
SUBJECT: Sensitive Information Posted to Personal Internet and Blog Sites

7. The Department of the Army and USAREUR will publish more specific guidance on these issues in the near future. We all must do our part now, however, to protect sensitive and classified information and ensure that it does not fall into the wrong hands.

8. This policy supersedes all previous related MNB (E) policies, is effective immediately, and will be posted on all unit bulletin boards.

9. Point of contact is the G6, LTC Fusco at DSN (314) 781-6600 or MAJ Levy, MNB (E) OPSEC manager at DSN (314) 781-6301.

Encl
ALARACT 156/2005
ALARACT DTG:141637Z



JOHN S. HARREL
BG, USA
Commanding

DISTRIBUTION:
A